

Naval Information Warfare Center Pacific (NIWC PACIFIC)

PERFORMANCE WORK STATEMENT

TO: N66001-20-F-3501
TITLE: Readiness Safety Systems (RSS) Management, Analytic and Technical Support
DATE: 07/10/2020

1.0 SCOPE

This is a Performance Work Statement (PWS) for a level-of-effort service acquisition to provide operations and sustainment, technical management, and analytical support for operational safety and occupational safety and health activities to reduce preventable mishaps and risks across the Department of Defense (DoD). This support includes data warehouse implementation, data collection and analysis, reporting, maintenance, technical support, and, assessment for the Under Secretary of Defense for Personnel and Readiness, USD (P&R), Force Safety and Occupational Health (FSOH).

2.0 OVERVIEW

DoD civilian and military leaders recognize the importance of effectively integrating deliberate loss prevention methodologies into all operational and work processes. Through multiple forums including programming guidance, memorandums, policy, and congressional testimony, senior leaders have directed the Department to ambitiously pursue mishap reduction efforts using best practices and the latest advances in technology in order to increase force readiness. In the execution of the DoD mission, it is imperative that all members of the DoD community maintain a vigilant commitment to safety. The effectiveness and readiness of the force is enhanced by minimizing avoidable losses whenever possible. Loss of personnel and assets are reducing DoD operational readiness and costing the DoD approximately \$3 to \$7 billion annually due to such events as, aviation mishaps, ground accidents, civilian workers' compensation claims, motor vehicle accidents, and military injury treatments. These losses place a significant demand on the military healthcare system, reduce personnel availability, and diminish force readiness.

2.1 Background

In a memorandum dated July 16, 2018, "Realignment of Safety and Occupational Health Policy and Oversight Functions in the Office of the Secretary of Defense," the Deputy Secretary of Defense directed the re-alignment of operational safety from the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) to the USD(P&R), and designated the USD(P&R) as the Principal Enterprise Safety Official (PESO). The PESO is fully empowered as the senior policy advisor to the Secretary of Defense and lead for integrated safety assessment and reporting, trend analysis, and mishap and accident reduction and mitigation activities. Further, the DEPSECDEF realigned responsibility for policy and oversight of operational mishap safety programs, including aviation, ground, motor vehicle, afloat, and space, to the USD(P&R). As a follow up to this action, on April 10, 2019, the Acting DEPSECDEF directed the realignment of the occupational safety and health mission from USD(A&S) to USD(P&R). Further, the Assistant Secretary of Defense for Readiness was designated as the DoD Designated Agency Safety and Health Official (DASHO).

These actions consolidated operational safety and occupational safety and health under the USD(P&R), which creates greater coherence in the Department to include policy development, governance, and communication with the Military Departments and other DoD Components. To implement this direction, USD(P&R) is responsible for updating the pertinent DoD issuances, performing annual comprehensive safety and occupational health program management reviews, and chairing the Defense Safety Oversight Council (DSOC) as the senior DoD safety governance body. The FSOH office, under the guidance of the Deputy Assistance Secretary of Defense for Safety and Occupational Health, is responsible for advising the USD (P&R) on key military readiness and safety issues with the objective of ensuring ready and responsive military forces. Through its working groups and task forces, the DSOC identifies risks and promotes data informed decisions that mitigate operational safety and occupational safety and health risks within the DoD. The Contractor is responsible for supporting FSOH in all its operational safety and occupational safety and health mishap reduction efforts.

These efforts are targeted at reducing/mitigating and/or analyzing, tracking, and managing preventable mishaps while accruing readiness benefits within DoD. The status of these efforts is reported to and from the DSOC and the DSOC Integration Group (IG), chaired by the Assistant Secretary of Defense (Readiness), and the DSOC Working Groups and Task Forces during regularly scheduled meetings. The Force Risk Reduction (FR2) tool provides timely and actionable baseline injury, mishap, and compliance data, tracking of performance metrics, integration of new data, and reporting to all levels DoD-wide. FR2 allows for the evaluation of safety and readiness data, the development of new analyses, and the improvement of current metrics, processes, and analyses. Data to support these efforts comes from all available sources.

2.2 Systems Overview

The DSOC is chartered to provide governance on DoD-wide efforts to reduce mishaps, which ultimately affects DoD readiness. Data must be collected, analyzed, and made available in order to identify impacts to DoD's readiness posture.

This effort includes the data collection and reporting of actionable data that is used to support decision and risk analysis, management, and resource allocation, identification and implementation of targeted mitigations to reduce risks inherent in daily operations, and reduction of unexpected and unintentional negative consequences that erode readiness/operational capacity. This effort also includes the setup, operation and maintenance, engineering, integration, implementation, testing, system documentation, and training of the FR2 tool, related enterprise information and data projects, and other mitigations focused on supporting the DSOC and FSOH's safety program. The FR2 tool is the focal point to support the information gathering, reporting, trending, and analysis. FR2 provides timely and actionable baseline injury, mishap, and compliance data, tracking of performance metrics, integration of new data originating from the initiatives, and reporting to all levels DoD-wide. FR2 allows for the evaluation of safety and readiness data, the development of new analyses, and the improvement of current metrics, processes, and analyses. Data to support these efforts comes from all available sources. In addition, other IT tools are used to collect and track information to support DoD installation's progress towards achieving an acceptable safety management system, such as the electronic Safety Management Systems (e-SMS) tool.

2.3 Pertinent Documents

The references listed below are applicable to the systems described in this PWS:

- USC Title 10, Section 117, Readiness Reporting System, and 482, 153, 193,167, 164
- DoDD 5124.02, 23 June 2008, Under Secretary of Defense for Personnel and Readiness (USD P&R)
- DoDD 8320.02, Data Sharing in a Net-Centric Department of Defense
- DoDI 6055.01, 14 October 2014, DoD Safety and Occupational Health (SOH) Program
- DoDI 6055.07, 6 June 2011, Mishap Notification, Investigation, Reporting, and Record Keeping
- Realignment of Safety and Occupational Health Policy and Oversight Functions in the Office of the Secretary of Defense Memorandum 16 July 2018
- DSOC Charter, 10 April 2019
- Safety and Occupational Health Oversight Functions Memorandum 10 April 2019
- OSHA 29 CFR 1960, Basic Program Elements for Federal Employees OSHA and Related Matters

Reference	URL/Location
DoDD and DoDI	http://www.dtic.mil/whs/directives/index.html
USC Title 10, Section 117	http://www.gpo.gov/fdsys/granule/USCODE-2011-title10/USCODE-2011-title10-subtitleA-partI-chap2-sec117
OSHA 29 CFR 1960	https://www.osha.gov/pls/oshaweb/owastand.display_standard_group?p_toc_level=1&p_part_number=1960
DSOC Charter	Available Upon Request

3.0 TECHNICAL REQUIREMENTS. The Contractor shall perform the following under this task order. Progress shall be reported to the Government in monthly status reports. Report shall include, at a minimum, technical progress made for each objective for that month, plans for the next reporting cycle, and financial update. Note that any Electronic and Information Technology (EIT) delivered under this task order shall incorporate the applicable EIT Section 508 Accessibility Standards (36 CFR Part 1194).

3.1 General Requirements

3.1.1 Description. The Contractor shall provide technical engineering and other support required to ensure the operational readiness and safety implementation to support the operations and maintenance of FR2 and technical support for Mishap, Readiness, Risk, Operational Safety and Occupational Safety and Health, and Programming and Assessment Data and Analysis. The Contractor shall perform the interface and coordination efforts necessary to facilitate data sharing and synchronization of data analysis. Technical Management includes coordination of FR2 technical operations, system enhancement, and information assurance. This function includes: compliance assurance, technical project management, human resource allocation, network operations supervision, IT resource management, partner coordination, IA governance, configuration change control management, system development life cycle oversight, data architecture, system and business requirements, and disaster recovery.

3.1.2 Deliverables.

- Monthly Status Report (CDRL A001)
- Contract Summary Report (CDRL A002)
- Management Plan (CDRL A012)
- Integrated Program Management Report (IPMR) (CDRL A013)
- Contractor Roster (CDRL A015)

3.2 Mishap, Readiness, Risk, Health and Resilience Data Warehouse Sustainment and Operations

3.2.1 Description. The Contractor shall maintain IT-based tools, data warehouse(s), and databases to use, merge, and analyze data for the purpose of providing information in a clear, concise, and coherent manner via various presentation methodologies. The Contractor shall support the development and updates of data use agreements and gather data from multiple sources that have the potential to impact force readiness. The Contractor shall provide maintenance to recurring reports and processes, as well in the execution of unique ad-hoc analytic tasks. The Contractor shall ensure FR2 has the correct organizational structure to drill down thru the commands to lowest units for all Services. The Contractor shall support FR2 as a data warehouse that maintains database tables, views, indexes, scripts, cubes, and reporting structures while ensuring modern software is used. This function includes: requirements review, database modeling, unit testing, performance tuning, and data mining analysis.

3.2.1.1 Requirements Collection and Management, Configuration Control Board (CCB)

The Contractor shall coordinate with the Government and participate in the FR2 Configuration Control Board (CCB) process. The Contractor shall work with the FR2 stakeholders and enterprise leads to collect and understand their requirements and business processes for analyzing and evaluating the integrated FR2 data, defining key performance indicators, reporting trends and using data to identify the root causes of various injuries and mishaps across the Department.

The Contractor shall establish and maintain detailed business rules for collection and integration of data through the life cycle of the program to ensure the FR2 warehouse is mapped accurately and reliably. The Contractor shall provide the capability to display automated high level and detailed reports and dashboards for leadership and reporting tools for end-users DoD-wide. Definitions must be consistent across DoD and drill-down capability must be available for all levels of the data.

3.2.1.2 Data Collection and Warehousing

The Contractor shall collect personnel, organizational, installation, financial, aviation, deployment, medical treatment, workers' compensation claims, casualty, accident reports, and other data such as problematic behavior information to provide to all levels of the Department for analysis. Information to be collected includes, but is not limited to, safety related data from the Army, Navy, Marine Corps and Air Force as well as fatalities, and personnel data for active duty, reservists, and civilian personnel. Currently, FR2 consumes data from the following providers:

- Defense Manpower Data Center (DMDC); Personnel, Deployment, Activation
- Defense Finance Accounting Service (DFAS) – Civilian Payroll Data
- Defense Civilian Personnel Advisory Service (DCPAS); Workers' Compensation Claims
- Defense Enrollment Eligibility Reporting System (DEERS)
- Defense Health Affairs; TRICARE Military Medical Treatment Claims
- Air Force Safety Automated System (AFSAS); Accident Reports
- US Army Safety Management Information System (ASMIS); Accident reports
- US Navy Web Enabled Safety System (WESS); Accident Reports
- USAF Transportation Command Regulating Command and Control Evacuation System (TRA2CES); Patient Movement Data
- Service Mortuary Affairs Centers
- Service Problematic Behavior Related Data
- Defense Casualty Information Processing System (DCIPS)
- Global Force Management Organization Server; Unit Structure (chain of command)
- Real Property Index; Installation Properties

The Contractor shall extract data, stage, transform, and load into the data warehouse and online analytical processing (OLAP) cubes after collection. Operations will be performed as needed by source (monthly at a minimum) and should yield approximately 350 million records for aggregated and drill-down data analysis. The total data warehouse currently stands at 172 gigabytes. New source data may be requested for integration into FR2 during the period of performance. Classified data may also be requested for integration on a potential FR2 SIPR.

3.2.1.3 Data Updates and Releases

The Contractor shall release data updates at least once per month and ensure that all User Interface/Report updates are provided with the associated documentation and instructions; and that all reports displaying are working correctly. Note: civilian lost time data should be updated every two (2) weeks based on the DMDC schedule.

3.2.1.4 Data Conformation and Integration of Business Rules

The Contractor shall process, conform, integrate, and fuse source data to enable accurate reporting, baseline trends, and root cause assessments. The Contractor shall integrate all data sets and all required fields to ensure in-depth analysis can be conducted by analysts and end-users. Business rules and requirements will also take into consideration the need to brief the highest levels within the DoD, ensuring data is accessible, accurate, reliable, and timely based on substantiated facts and trends.

This data should be readily available in easily usable reporting and dashboard tools to be used by multiple types of end-users. Easily usable refers to the ability for the target audience (OSD, Military Department and Agency leaders, analysts, epidemiologists) to achieve their goals with effectiveness and efficiency.

3.2.1.5 Business Intelligence

The Contractor shall provide tested reporting tools including instructions for use by data analysts and other Government POCs to conduct in-depth analysis and trending of data across and between multiple data sets. The Contractor shall maintain tested and proven software functionality that allows end-user reporting and data mining capability along with high level and strategic dashboard displays and reports.

The Contractor shall provide tools to monitor and quantitatively evaluate mishap impact data, allowing data to be compared and contrasted, as well as exported or otherwise manipulated similar to statistical software which may be used by FR2 analysts and ensure all source data is usable and compatible with the existing OSD (P&R) FSOH tools.

3.2.1.6 Data Requests and Queries

The Contractor shall respond to data requests from the OSD (P&R) FSOH office, the DSOC, and related working groups and task forces, along with monthly metrics reporting status of the DoD mishap reduction goal and analysis that prepares the OSD leaders for unit and installation assessment visits, with complete, accurate and reliable data. Certain data, such as the military injury medical treatment data from TRICARE, shall be made available to the Services in order to be compared against Service mishap data. This may require web service feeds or flat files to be updated on a minimum monthly basis.

3.2.1.7 Data Integrity and Quality Assurance

The Contractor shall follow industry standard processes and procedures to ensure that the Government receives accurate and reliable data to support the identification of trends and any DoD mishap reduction goals. The Contractor shall ensure data is:

- Accurate
- Complete
- Relevant
- Consistent across all sources
- Reliable
- Appropriately presented
- Accessible

The Contractor shall maintain data quality by performing regular periodic reviews, quality assurance reports, and updates. Quality assurance evaluates the quality of data and technical refresh. This function includes: checking the quality of the data files received from the source providers, tracking key quality indicators with the data received each month, testing software deliverables on each of the product delivery environments, and verifying the quality of change in supporting applications.

3.2.1.8 Support Integration of Safety-Related Projects and/or Tools

The Contractor shall provide support, when directed by Government, with hosting efforts for other DSOC and readiness related projects and input tools where applicable. Support areas include but may not be limited to the Medical Evacuation Tracking interface, and the Near Miss Reporting System. The Contractor shall support OUSD (P&R) FSOH with the identification and prioritization of other projects and tools and provide data analysis for requests related to these and other projects managed under other contracts.

3.2.2 Deliverables.

- Briefing Material (CDRL A003)
- Report, Record of Meeting/Minutes (CDRL A004)
- Technical Report –Study / Services (CDRL A005)
- Computer Software Product End Items (CDRL A006)
- Operational Concept Document (CDRL A008)
- Software Test Plan (CDRL A009)
- Software Version Description (CDRL A010)
- Software User's Manual (CDRL A011)

3.3 Programmatic, Analytical, and Administrative Support, Assessment, Data and Analysis, and Mishap Reduction Mitigations

3.3.1 Description. The Contractor shall provide qualified technical support and personnel to perform data analysis on the execution of data-driven decisions of the DSOC to promote accident and injury reduction and improvements to risk behaviors.

3.3.1.1 DSOC Coordination and Support

The Contractor shall provide support to OUSD P&R and the FSOH office with requirements collection, analysis of alternatives, technical evaluation, execution, and reporting of technical projects. These projects shall improve readiness and availability of military and civilian workforce in the areas of operational safety, occupational safety and health, government tactical and private motor vehicle safety, aviation safety, ergonomics, human factors, compliance

assistance, and other enterprise safety risk management and loss reduction efforts. These efforts require data collection and analysis to: establish a baseline, identify key performance parameters, determine effectiveness, develop a business case, calculate return on investment, conduct surveys, collect feedback for continuous improvement, and ensure available data is accessible via FR2.

The Contractor shall coordinate and execute enterprise data information and data projects to reduce mishaps and mitigate risks identified through the data analysis for the DSOC, as directed by the Government. Projects may include the following efforts, or other similar efforts in support of the Department's mishap reduction objectives:

- Providing an effective, non-intrusive process and associated methodology for importing, merging and synchronizing operational safety data and information being submitted from high-side sources into the FR2 database.
- Providing necessary support to feed the military injury treatment data feeds to the Service Safety Centers.
- Provide support for updating the existing mishap common data elements and business enterprise architecture and updating the related data feeds to FR2, ensuring data collected assists in overcoming uncommon data across the DoD.
- Develop and conduct surveys and questionnaires to collect target audience cultural and perception data, as feasible, merge data with FR2, analyze data and report results.
- Use data analysis and recommendations to improve readiness and availability of civilian workforce through policies, programs, legislative changes, and investments for reducing civilian injury compensation such as return to work initiatives and streamlined and expedited claims.
- Use data analysis and recommendations to improve readiness and availability of military and civilian workforce through acquisition policies, procedures, standards for all systems (aviation and weapon systems and human integration systems) to address safety requirements.
- Recommend ways to ensure milestone decision reviews and interim progress reviews address safety performance.
- Provide analytic support, such as changes to organizations from joint base actions, identifying orphan or unknown unit identification codes and recommending to the system database analyst the proper placement of the units in the DoD unit organization hierarchy reference table.
- Support integration of new data based on results of DSOC Task Forces, such as but not limited to the mishap classification Task Force and leading indicators Task Force.
- Provide support for updating existing DoD FSOH related policies.

The Contractor shall provide support with the planning and execution of DSOC meetings which take place approximately two (2) times per 12-month period, as well as other related meetings that may occur throughout the year, such as the DSOC Integration Group (approximately four (4) times per 12-month period), the DSOC Steering Group (approximately 10 times per 12-month period), and DSOC Working Group and Task Force meetings (schedules to be determined by Chairs). The Contractor shall be required to reserve facilities, plan agendas and speakers, maintain rosters and attendance lists, maintain protocols, prepare read-ahead and presentations, and coordinate Defense Connect Online or Video Teleconferencing

and after-action items and minutes, as requested. The Contractor shall coordinate with DoD analytic working groups that use the FR2, DSOC, military and civilian injury working groups, and other related committees. The Contractor shall work with the Government to support and sustain the increasing FR2 user base.

3.3.1.2 Office of Drug Demand Reduction (ODDR)

The Contractor shall provide support to the ODDR, and related efforts through analysis, and on-site program and project support, including establishing and maintaining ODDR annual and other data reports and potentially new data feeds to FR2. The contractor shall support coordination with DMDC regarding positive drug test matching data. The Contractor shall improve readiness and availability of military and civilian workforce through analysis, tracking, and reporting of data on wellness programs such as ODDR, traumatic brain injury, post-traumatic stress, and other problematic behavior and health of the Force issues. The Contractor shall incorporate data into OSD metrics as required.

The Contractor shall support collection and analysis of information in support of the ODDR reporting requirements. The Contractor shall summarize data analysis and prepare reports, briefings, and displays that allow Government personnel to coordinate the budgeting and execution tasks associated with the program. In the event limited access to Planning, Programming, Budgeting, and Execution (PPBE) data may be required to support ODDR and FSOH, the Contractor shall be required to complete written agreements that authorize access to the information.

3.3.1.3 Interface with Service Safety Centers and Minimum Data Requirements

The Contractor shall support the DSOC efforts with the Service Safety Centers, including to meet the Common Data Elements Requirements (CDE) defined in Department of Defense Instruction (DoDI) 6055.07. Unifying mishap data under CDE semantics will enable true cross-service safety data analysis. The Contractor shall integrate each Service's data elements into the FR2 data warehouse to allow for cross-service analysis and unified data integration with other related safety sources, thus creating a more complete understanding of the mishap and related events, leading to more complete DoD mishap trending and analysis. The Contractor shall also assist with human factors coding and analysis of mishap data.

3.3.1.4 Data Analysis and Reporting

The Contractor shall provide technical support to the DSOC working groups and task forces that use FR2 data. The Contractor shall provide trending and statistical analysis of the integrated FR2 data to identify significant accident causes or individual events that serve as the foundation for recommendations presented at key decision briefings, reports, and meetings, such as the DSOC, DMAG, wellness reviews, and other related forums.

The Contractor shall provide support to OUSD (P&R) FSOH and the DSOC with data collection and analysis, business case and return on investment calculations, development, and conduct of surveys, and collection of feedback for continuous improvement.

The Contractor shall complete mishap reporting per DoDI 6055.07 with appropriate structure and content of DoD personnel, medical treatment (ICD 9 and 10 codes), and financial data

constructs, as well as DoD organizational structure as contained in the Service structures. The Contractor shall apply analytical techniques such as the Barrell Matrix, rates, regression analysis, chi square, and developing cost benefit analysis, as required. The Contractor shall analyze and interpret integrated data as it applies to the operational environment.

The Contractor shall recommend, update, maintain, track, and report OSD related safety metrics on a minimum monthly basis using FR2 data. The Contractor shall recommend, develop, collect and track any new metrics as required by the Government. The Contractor shall provide maintenance support to OUSD (P&R) FSOH websites, including DENIX as required by the Government. The Contractor shall maintain data reporting and dashboard capabilities, ensuring information is retrievable quickly and with as few key strokes as feasible. Links and buttons shall be distinctive, use clear language, and allow users to build on their knowledge without deliberate effort. Tool tips and definitions shall be readily available to users.

3.3.2 Deliverables.

- Briefing Material (CDRL A003)
- Report, Record of Meeting/Minutes (CDRL A004)
- Technical Report – Study/Services (CDRL A005)

3.4 Safety Management Systems (SMS) Operations and Technical Support

3.4.1 Description. The Contractor shall provide technical support for operation and improvement of the DoD Safety Management Systems (SMS), including but not limited to programs such as OSHA's Voluntary Protection Programs (VPP) and Army Star, as well as other Service SMS programs, and industry programs such as ANSI Z-10 and ISO 45001. The objective is to provide an integrated framework and comprehensive approach to DoD safety and occupational health systems management to improve safety program performance at DoD installations. This includes use of IT tools to establish, track, and analyze input and output metrics by which success is measured.

The Contractor shall assess an installation's compliance with the OSHA VPP or other SMS established criteria. This assessment is a means for DoD to expand the Service's ability to meet the requirements in DoDI 6055.01 to achieve a world class safety program in the form of a safety management system. These activities shall include operation of the Safety Management (SM) Center of Excellence (CX) and an electronic SMS (e-SMS) tool and demonstration of new and innovative information technologies, tools and best practices.

3.4.1.1 Safety Management Center of Excellence Support

The Contractor shall provide centralized SM support via a Safety Management Center of Excellence to support the more than 400 DoD sites in various stages of progress towards their completion of a SMS. The Contractor shall provide on-site and remote support. This includes a series of data collection activities, policy/document reviews, meetings with key personnel from management/command through the workers and Contractors, group education, and various types of interviews.

The Contractor shall support the data collection and compare the data to the requirements for the SMS. The Contractor shall prepare an installation/site gap analysis for the variances. The

Contractor shall assist the installations and sites input the data into the e-SMS tool, which provides a calculation of the percent complete the site is along the path towards obtaining an OSHA VPP Star, Army Star, or other DoD SMS objectives.

The Contractor shall work with the sites and installations to gather the missing elements and enter these data into the e-SMS tool as applicable to document the progress, actions, or activities taken by the site to meet individual elements. The Contractor shall conduct a preliminary assessment prior to a final third-party certification for a site and/or participate with the third-party certification activities.

The Contractor shall provide proactive communications and coordination with Government stakeholders at all levels (from service/agency to installation). This includes providing information that facilitates the VPP Special Government Employees attaining and maintaining their OSHA certifications.

The Contractor shall facilitate and support meetings, workshops, conferences, webinars, and other forums for data collection and analysis, education, training, outreach, and communicating with sites and stakeholders.

The Contractor shall provide technical remote support to the Services and Major Commands working to implement safety management systems to the Services and Defense Logistics Agency, as well as other DoD agencies.

3.4.1.2 Electronic Tools Hosting and Operations

The Contractor shall support hosting, and provide operations and maintenance of the related electronic tools, databases, training, and informational portals. The Contractor shall provide seamless operation and maintenance of the e-SMS tool to ensure it is meeting DoD installation requirements towards meeting their safety management system objectives. The objective of an SMS is to provide a structured management approach to control safety risks in operations. Effective safety management must take into account the organization's specific structures and processes related to safety of operations. The ultimate goal is to prevent all lost time accidents at the site. The e-SMS tool may be used to enter, monitor, track, and update the information. The Contractor shall assist the sites and installations who input information into the e-SMS tool during the work week

3.4.1.3 DSOC Safety and Occupational Health Management Systems Working Group Support for DoD SMS Activities

The DoD Safety and Occupational Health Management Systems Working Group (SOHMS WG) will support the requirements for DoD SMS work. The Contractor shall assist the Government by operating the SMCX as a DoD-wide resource for implementing Safety and Health Management Systems resulting in reduced injury and illness rates as well as reductions in lost work day rates that support the DSOC mishap reduction objectives and the DoD and any related Congressional initiative metrics. The Contractor shall provide support for regular updates, briefings, and participation as needed in SOHMS WG meetings related to SMCX activities.

3.4.1.4 On-Site Visits Support

The Contractor shall assess an installation's compliance with the OSHA VPP or other SMS

established criteria by conducting on-site visits in the most efficient and effective manner possible. The Contractor shall apply OSHA VPP concepts and certification processes and criteria, comply with OSHA laws and regulations (29CFR1960), and maintain injury and illness rates as compared to industry averages in order to assess sites and provide analysis of site readiness and gaps from the criteria, as well as experience with other SMS including but not limited to Army Star, ISO 45001, and ANSI Z10.

The Contractor shall work with the Service POCs to coordinate and finalize the details of the site visits and the nomination of new sites annually. Services will finalize the new participating sites and the prioritization of site visits each year. The Contractor shall inform the Service POCs and RSS Government Program Manager of changes to schedules and site preparedness. This information will be consolidated and updates provided to the RSS Government Program Manager.

Types of visits with typical number of travelers include:

- Baseline Assessment (up to 3 analysts)
- Stage Completion/Implementation Visit (up to 3 analysts)
- Application Readiness Assessment (3-4 analysts)
- Recertification Assessment (3-4 analysts)
- General/Technical Assistance Visit (up to 3 analysts)

A Baseline Assessment is conducted for each newly nominated site. In coordination with Service/Agency and Site leadership the Contractor shall:

- identify all process owners to be included in the assessment,
- identify all operations to be included during the assessment,
- identify and review data needed to perform a Baseline Assessment to include written safety and occupational health programs, instructions, regulations etc. This documentation should include programs that are site or major command specific,
- prepare and provide written programs and processes for emergency services (fire services fire prevention, security, medical response, emergency preparedness, etc.),
- prepare and provide written programs and processes regarding the execution of preventive maintenance on the site,
- prepare and provide written safety and occupational health programs, and
- disclose OSHA incident rates.

As required, the Contractor shall upload a Stage 1 web-based Action Plan via the e-SMS Tool for the sites to continue SMS Implementation after the Baseline Assessment.

Stage Completion/Implementation Visits are conducted once sites have completed all Stage 1 or 2 actions. The Contractor shall verify authenticity of the completed actions if a site has completed Stage 1 actions as well as provide insight to strategies for completing Stage 2 actions. The Contractor shall verify authenticity of the completed actions as well if a site has completed Stage 2 actions as provide insight to strategies for completing Stage 3 actions and preparing for the VPP or other application process. The Contractor shall provide an Action Plan in either case, via the eSMS Tool as applicable, for reducing or eliminating the identified gaps in the stage.

Application Readiness Assessments are conducted once a site is deemed completing the criteria

and before OSHA or other external evaluations commence. The Contractor shall thoroughly review all criteria to ensure a successful OSHA/Army Star/other SMS evaluation. A recertification assessment is required for any site commencing an OSHA, Army Star, Navy OCONUS recertification.

General/Technical Assistance visits are provided to sites requesting additional support in implementing and sustaining their SMS efforts. The Contractor shall provide technical assistance onsite including but not limited to, leadership training, assessor and/or implementation training, regulatory compliance assistance, and supervisor and/or employee awareness training. General/Technical Assistance Visits may also include support to FSOH at annual SMS-related events such as conferences or training sessions.

3.4.1.5 End User Support

The Contractor shall provide proactive communications and coordination with Government stakeholders at all levels (from Service/agency to installation). The Contractor shall facilitate and support meetings, workshops, conferences, webinars, and other forums for data collection and analysis, education, training, and communicating with sites and stakeholders, and provide technical remote support to the Services and Major Commands working to implement safety management systems to the Services and Defense Logistics Agency, as well as well as other DoD agencies.

3.4.2 Deliverables.

- Briefing Material (CDRL A003)
- Report, Record of Meetings/Minutes (CDRL A004)
- Technical Report – Study/Services (CDRL A005)
- Computer Software Product End Items (CDRL A006)
- Training Materials (CDRL A007)
- Operational Concept Document (CDRL A008)
- Software Test Plan (CDRL A009)
- Software Version Description (CDRL A010)
- Software User's Manual (CDRL A011)
- Management Plan (CDRL A012)
- Integrated Program Management Report (IPMR) (CDRL A013)

3.5 Lifecycle Support

3.5.1 Configuration Management

The Contractor shall establish a configuration management process for documenting and maintaining consistency of traceable requirements, source code, database and design details, and operational information, and other life cycle artifacts. The configuration management process will include the ability for evaluating, coordinating, approving or disapproving, and implementing changes used to construct and maintain software systems and data warehouse specifications. The Contractor shall provide the Technical Representative with reports on engineering changes and their status, baseline configuration, and changes to the baseline configuration. The configuration management system and access to all associated work products, requirements, and work items, will be readily accessible to members of the safety community including Government and other Contractors.

The Contractor shall update and maintain all system artifacts as required by the Government. The Contractor shall comply with all DoD related documentation, including requirements to operate within the DoD Information Technology (IT) framework, DoD Risk Management Framework, data use agreements, a detailed FR2 user's guide, and documented business rules for all data integration, data dictionaries, and other information necessary to ensure standard software documentation is readily available.

The Contractor shall securely acquire data from the source providers, load the data, identify and track the configuration items in scope for a given application version, manage the software source control system, assemble the components of an application version, run the programs that process data, process cube structures, backup of all software deliverables, build the system test server, and deploy the application to the secured production site as a formal product release. All software products developed are property of the Government.

3.5.1.1 Systems Engineering and Integration

The Contractor shall provide systems engineering and integration support using Government approved configuration requirements. The Contractor shall configure and integrate FR2, and any other related information technology systems using the appropriate Government approved software and hardware.

The Contractor shall participate in system requirements analysis and functional requirements definition. The Contractor shall use Government approved methods, processes, and tools for system requirements collection, analysis, design, testing, installation, integration, documentation, security, and management. The Contractor shall develop, publish, and maintain schemas and data base dictionaries for the systems. The Contractor shall recommend software integration approaches which describe program modules, classes, objects, databases, Graphic User Interface displays and reports needed to successfully implement the application program functional requirements.

The Contractor shall provide technical and analytical services in support of databases, process improvement, integration and system support emphasizing system security. The Contractor shall provide high-level design of network architectures, describing hardware configurations, software capabilities, and connectivity. The Contractor shall provide high-level design of application software and data interfaces. The Contractor shall create and register schema at the Government-approved registry when required. The Contractor shall participate in meetings with Government commands and activities and support the resolution of schedule issues resulting from coordinating implementation policy.

The Contractor shall provide:

- Daily systems health check
- Security patches
- Error log review
- Configuration change testing
- Backup verification
- Server room management
- Network switch management

- Hardware maintenance
- Vulnerability scanning
- System administration
- Risk Management Framework (RMF) and cybersecurity control compliance
- Maintenance of mission-critical applications

This contract provides for systems engineering for RSS Management, Analytic and Technical Support. The parties recognize that by the Contractor providing this support, a potential conflict of interest arises as defined by FAR 9.505-1.

3.5.1.2 System Administration and Database Operations and Maintenance

The Contractor shall provide systems administrative services for the FR2 and related safety management system tools used in support of OUSD (P&R) FSOH projects and programs. The Contractor shall perform backups of the production system including:

- Full nightly system backups for all virtual machines to SAN (storage area network)
- Archived weekly system image archives to a separate NAS (network attached storage)
- Archived backup copied to an offsite backup storage unit
- Full database backups nightly for all SQL databases to SAN

The Contractor shall also provide database administration on table structures, access to data, replication support, disaster recovery procedures and backups. The Contractor shall also:

- Maintain user accounts
- Pull data from source systems on at least a monthly basis
- Diagnose issues with source data files and resolve with data provider

3.5.1.3 Production Environment Support

The Contractor shall provide support to the FR2 production environment:

- Manage hardware and software operation within accredited enclave
- Maintain cyber security controls within the DoD risk management framework and perform scans monthly and as needed to ensure compliance
- Assure encryption and other security standards are integrated (e.g. PKI, CAC)
- Ensure backups are effective and disaster recovery plans are updated
- Support and troubleshoot data service connections (e.g. SOA, SFTP, etc.)
- Provide immediate assistance for service interruptions during standard business hours
- Manage Microsoft Active Directory
- Manage user accounts and respond to user requests
- Interface with hosting network authorities in problem resolution
- Update the site with the appropriate marketing materials & other pertinent information

3.5.1.4 Implementation and Deployment Environment Support

The Contractor shall provide support to the RSS implementation and deployment environment:

- Manage hardware and software operation within the development network supporting implementation, testing, and staging
- Assure boundary integrity from isolated HIPAA network
- Assure encryption and other security standards (e.g. PKI, CAC)
- Maintain cybersecurity controls and perform monthly scans
- Ensure backups are effective and disaster recovery plans are prepared

- Provide immediate support for service interruptions
- Manage Microsoft Active Directory
- Manage user accounts and respond to user requests
- Perform hardware maintenance on Government-owned systems
- Perform hardware and software asset management on Government-owned systems
- Maintain program support systems, including document repository, source code repository, and issue tracking systems

The Contractor shall ensure that the systems allow authorized users to easily change what information users can view or update. FR2 access shall be available 24 hours per day, seven (7) days per week. Response time must meet Government requirements specified below:

Attribute	Development Threshold	Development Objective
Operational Availability	Average 23:30 hours daily availability over a 30-day period.	Threshold=Objective
New Accounts	Performed within 24 hours of request	Threshold=Objective
Changes to User Role	Performed within 24 hours of request	Threshold=Objective

3.5.1.5 Information Security (INFOSEC)

The Contractor shall ensure and maintain proper IT cybersecurity and management services, including technology controls and features that protect all of the FR2 information in compliance with Government policies and regulations in addition to incorporating technology safeguards to proactively protect the system and its data from security breaches or policy violations of any kind. The Contractor shall participate in implementing and/or supporting DoD and local site INFOSEC policy and guidance. The Contractor shall provide INFOSEC planning and maintenance services including update of security documentation to reflect new or changed physical configurations and security requirements.

The Contractor shall:

- maintain the capability for users to register and access the FR2 site via CAC sign on
- ensure systems in this PWS are capable of limiting access to information based on the customers need to know
- ensure all Service Oriented Architecture (SOA) applications will support integrated Identity Management, Permissions Management and Digital Rights Management ensuring that adequate confidentiality, availability and integrity are provided
- assist the Government with production site cybersecurity requirements, to include ensuring all accredited environments are audited regularly and are compliant with the latest Security Technical Implementation Guides (STIGs) / Security Readiness Review (SRR) / Security Requirements Guide (SRG) / Security Automation Content Protocol (SCAP)
- perform weekly audit log reviews
- perform monthly vulnerability scans
- comply with USCYBERCOM Task Orders
- perform monthly cybersecurity compliance checks (or when requested by the USA/CRC)
- conduct security impact assessments every six (6) months (or when requested by

- the USA/CRC)
- perform cybersecurity artifact updates every six (6) months (or when requested by the USA/CRC)
- prepare for certification and accreditation (CDRL A016)

3.5.2 Deliverables.

- Briefing Material (CDRL A003)
- Report, Record of Meetings/Minutes (CDRL A004)
- Technical Report – Study/Services (CDRL A005)
- Computer Software Product End Items (CDRL A006)
- Training Materials (CDRL A007)
- Operational Concept Document (CDRL A008)
- Software Test Plan (CDRL A009)
- Software Version Description (CDRL A010)
- Software User’s Manual (CDRL A011)
- Management Plan (CDRL A012)
- Integrated Program Management Report (IPMR) (CDRL A013)
- Information Systems Accreditation Documentation (CDRL A014)

3.6 Training Support

3.6.2 Description. The Contractor shall provide training to users of fielded systems and provide readiness-related and personnel risk reduction training resulting from the results and analysis from pertinent safety-related projects. The Contractor shall develop curriculum, present, and maintain training course materials and training manuals to support FR2 and all related projects. Training includes instructor-led and web-based learning.

The Contractor shall support FR2 training and safety community training and education events. The Contractor shall participate in administrative tasks such as scheduling classes, tracking student loading and instructor assignments, and processing payments, receipts and invoices. The Contractor shall coordinate and implement events to share lessons learned, recommendations, and present a demonstration of results to DoD leaders, and provide communications support by working with Service and Department public affairs and other relevant media outlets.

3.6.3 Deliverables.

- Briefing Material (CDRL A003)
- Report, Record of Meetings/Minutes (CDRL A004)
- Technical Report – Study/Services (CDRL A005)
- Training Materials (CDRL A007)

3.7 Help Desk and Trouble Call Support

3.7.1 Description. The Contractor shall provide 24 hour/5 day a week (Monday through Friday) help desk/support center and support training. This includes requirements for monthly (or as

needed) training on the FR2 application. The Contractor shall provide help desk support by responding to trouble calls and providing technical and administrative support / information for FR2. Response to trouble calls shall be provided within one business day. The Contractor shall provide a response record log and respond via the military email system or by any means available. The help desk shall provide assistance in uploading, generating queries, and downloading information.

3.7.2 Deliverables.

- Briefing Material (CDRL A003)
- Report, Record of Meetings/Minutes (CDRL A004)
- Technical Report – Study/Services (CDRL A005)
- Training Materials (CDRL A007)

3.8 Management Support

3.8.1 Description. The Contractor shall develop presentations, reports, point papers and other documentation in support of the tasks described in this PWS. Products shall be delivered in a timely manner.

The Contractor shall support the development of executive-level presentations, information for trip books, and graphical representations of current DoD safety programs, data, and metrics.

The Contractor shall participate in and document working group meetings and conferences to help determine requirements, discuss implementation issues, conduct reviews, and other project related purposes when directed by the Government. The Contractor shall submit meeting minutes/trip reports documenting the results of these meetings within five (5) business days after the end of the meeting/trip.

The Contractor shall participate in system reviews required by the Government. The Contractor shall participate in project review meetings and report project review report when required by the Government.

The Contractor shall conduct and/or attend weekly Technical Interchange Meetings (TIMs) to facilitate the exchange of technical information and enhance effective communication among the interested parties authorized by the Government.

The Contractor shall use e-mail for administrative coordination issues. Classified (up to SECRET) information can be transmitted via SIPRNET e-mail.

3.8.2 Deliverables.

- Briefing Material (CDRL A003)
- Report, Record of Meetings/Minutes (CDRL A004)
- Technical Report – Study/Services (CDRL A005)

3.9 Staffing and Key Personnel. The contractor shall provide personnel that meet or exceed the minimum requirements identified in task order attachment 3. Additionally, the contractor shall provide key personnel as follows:

- (a) The offeror agrees to assign to this contract those key personnel for positions listed in paragraph (d) below. No substitutions shall be made except in accordance with this text.
- (b) The offeror agrees that during the first 60 days of the contract performance period no personnel substitutions will be permitted unless such substitutions are necessitated by an individual's sudden illness, death or termination of employment. In any of these events, the contractor shall promptly notify the Contracting Officer and provide the information required by paragraph (c) below. After the initial 60 day period, all proposed substitutions must be submitted in writing, at least 14 days in advance of the proposed substitutions to the contracting officer. (Note: onboarding may take more than 14 days if a security clearance is required.) These substitution requests shall provide the information required by paragraph (c) below.
- (c) All requests for approval of substitutions under this contract must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitutions. They must contain a complete resume for the proposed substitute or addition, and any other information requested by the Contracting Officer or needed by him to approve or disapprove the proposed substitutions. All substitutions proposed during the duration of this contract must meet minimum personnel qualifications identified in the contract. The Contracting Officer or authorized representative will evaluate such requests and promptly notify the contractor of approval or disapproval thereof in writing.
- (d) List of Key Personnel

Labor Category	Employee Name
Program Manager	(b)(4)
Program Manager	(b)(4)
Senior Software Engineer	(b)(4)
Senior Software Engineer	(b)(4)
Principal Safety Management Systems Pro	(b)(4)
Principal Safety Management Systems Pro	(b)(4)
Principal Safety Management Systems Pro	(b)(4)
Principal Safety Management Systems Pro	(b)(4)
Principal Safety Management Systems Pro	(b)(4)
Principal Safety Management Systems Pro	(b)(4)
Principal Safety Management Systems Pro	(b)(4)
Principal Safety Management Systems Pro	(b)(4)
Principal Safety Management Systems Pro	(b)(4)
Senior Systems Analyst	(b)(4)
Sr Operations Research/Data Analyst	(b)(4)

Labor Category**Employee Name**

Sr Operations Research/Data Analyst
Sr Operations Research/Data Analyst
Sr Operations Research/Data Analyst
Subject Matter Expert
Subject Matter Expert
Subject Matter Expert
Program Manager
Subject Matter Expert
Senior Network Engineer
Senior Network Engineer
Sr Database Engineer
Sr Database Engineer
Senior Software Engineer
Senior Software Engineer
Data Warehouse Information Security Manager
Senior Systems Analyst
Sr Operations Research/Data Analyst
Data Warehousing Manager
Senior Systems Analyst
Subject Matter Expert

(b)(4)

(e) If the Contracting Officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated or have otherwise become unavailable for the contract work is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the Contracting Officer for default or for the convenience of the Government, as appropriate. In addition, if the contractor is found at fault for the condition, the Contracting Officer may elect to equitably decrease the contract price or fixed fee to compensate the Government for any resultant delay, loss or damage.

4.1 DELIVERABLES

4.2 Data Deliverables. Technical data and computer software deliverables shall be provided in accordance with the Contract Data Requirements List, DD Form 1423. All deliverables are subject to NIWC Pacific review and approval before final acceptance. All classified deliverables shall be protected and handled in accordance with standard security practices and procedures. The Contractor shall use e-mail for administrative coordination issues. Classified (up to Secret) information can be transmitted via SIPRNET e-mail.

5.0 SECURITY REQUIREMENTS. The work performed by the Contractor shall include access to Unclassified and up to Secret data, information, and spaces in accordance with the DD 254 attached to the order. The Contractor shall follow mandated procedures to ensure information access is limited to individual classification level (e.g. unclassified for any

individual without a SECRET clearance). The Contractor will require access to Secure Internet Protocol Router Network (SIPRNet). The Contractor shall be North Atlantic Treaty Organization (NATO) briefed and complete the derivative classification training prior to being granted access to SIPRNet; training is provided by the facility security officer.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the Commanding Officer, Attn: Foreign Travel Team, Naval Information Warfare Center Pacific, 4201 Pacific Highway, Old Town Complex 2, Room 1656, San Diego, CA 92110 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 30 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and Contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at <https://atlevel1.dtic.mil/at/>, if experiencing problems accessing this website contact ssc_fortrav@navy.mil. Forward a copy of the training certificate to the previous email address or fax to (619) 553-6863. SERE 100.1 Level A Code of Conduct training is also required prior to OCONUS travel for all personnel. SERE 100.1 Level A training can be accessed at <https://wwwa.nko.navy.mil>. Other specialized training for specific locations may also be required contact the SSC Pacific foreign travel team.

As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, Contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL); 2) the status of an employee's personnel clearance (PCL); 3) the proper safeguarding of classified information; 4) or an indication that classified information has been lost or compromised. Contractors working under SSC Pacific contracts will ensure information pertaining to assigned Contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the Contractor's operation while working under SSC Pacific contracts.

Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and Contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at <https://atlevel1.dtic.mil/at/>, if experiencing problems accessing this website contact: ssc_fortrav@navy.mil.

5.1 Operations Security. OPSEC is a five-step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or Critical

Program Information (CPI), and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD and OPSEC requirements and in accordance with the OPSEC attachment to the DD254.

5.2 Cyberspace Workforce. The Contractor shall meet the Cyberspace Workforce (CSWF) standards in accordance with 5205.02-M, and DoD 8570.01-M. Contractors who perform cybersecurity duties or functions, whether primary or additional, on DoD computer systems (stand alone or networked) shall meet the certification requirements for each category/ level/ and operation environment as required. IAM Level III certification is required for the Data Warehouse Information Security Manager.

The Contractor shall ensure that personnel accessing information systems have the proper and current IA certification to perform IA functions identified in section 3.5 of this PWS in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet applicable information assurance certification requirements, including (a) DoD-approved IA workforce certifications appropriate for each specified category and level and (b) appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions. Certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

The Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions, reporting current IA certification status and compliance using CDRL A015, Contractor Roster in the format prescribed by the COR. CSWF positions with privileged access and who perform information assurance duties or functions will be identified at the task order level in the performance work statement. These positions shall meet the background investigation requirements for each category/ level/ and operational environment as required by DoD 5200.2-R and DUSH HCIS Memorandum, November 4, 2010. See Information Technology Systems Personnel Security Requirements DD254 attachment for background check requirements. The Contractor shall identify document, track, and report certification status and shall report change in Contractor personnel or tasks that impact CSWF.

5.2.1 IA Function Description. The Contractor shall implement and maintain policies and goals that support the organization's IT needs. The Contractor shall ensure proper functioning of the information processing system and oversee necessary updates. The Contractor shall help business operations groups utilize information systems to improve their efficiency. The Contractor shall ensure computer equipment, hardware, and software is updated to meet organizational needs.

5.2.2 Deliverables.

- Monthly Status Report (CDRL A001)
- Report, Record of Meetings/Minutes (CDRL A004)
- Technical Report – Study/Services (CDRL A005)
- Contractor Roster (CDRL A015)

6.0 OTHER

6.1 Government Furnished Property (GFP). Computer hardware and communication infrastructure that are required to develop, support, and implement the system shall be Government Furnished Property (GFP) for work conducted on Government site or required in order to execute Government requests.

The Contractor shall furnish all professional, technical, and clerical personnel and services, software, materials, equipment and travel to conduct the necessary work that is off-site not covered in 6.1.2 or 6.1.3.

The Contractor shall identify, track, and report hardware and software Government Furnished Property/Government Furnished Equipment and any Contractor Acquired Property assets in the Contractor's possession to the Technical Representative. The Contractor shall periodically perform, record, and disclose physical inventory results. A physical inventory shall be performed upon contract completion or termination. The Contractor shall investigate and promptly furnish a written narrative of all incidents of loss, damage, destruction, or theft to the Government property administrator as soon as the facts become known or when requested by the Government.

The Contractor shall also report expiration of hardware and software warranties and licenses in a timely manner prior to actual expiration date.

6.1.2 Production Environment. The FR2 production environment is comprised of the following hardware and software, but this could be subject to change.

Software	Operating System	MS Windows Server 2012 R2 Standard (5 server)
		Windows Server 2016 Standard (32 cores)
		RedHat Enterprise Linux (2)
	Database	Microsoft SQL Server 2014 (4 cores)
		Microsoft SQL Server 2016 (8 cores)
	Web Services	Microsoft SharePoint 2013
	Tool	Solarwinds Server & Application Monitor
		Splunk Enterprise (1 GB/Day)

6.1.3 Implementation and Deployment Environment. The implementation/deployment environment shall be located at the Contractor site as Government Furnished Equipment.

Hardware	Servers	Dell PowerEdge R610
		Dell PowerEdge R610
		Dell PowerEdge R630
		Dell PowerEdge R630
		Dell PowerEdge R710
		Dell PowerEdge R710
		Dell PowerEdge R710
		Dell PowerEdge R710
		Dell PowerEdge R710
		Dell PowerEdge R710
	Server Device	Dell PowerEdge Rack Console 15FP
		Dell PowerEdge 2161 Remote Console (KVM)
		Dell PowerEdge Rack
		Crucial Technology 16GB PC3-12800 1600MHZ DDR3 240-Pin DIMM Dr X4
		Crucial Technology 16GB RAM (7)
		Crucial DDR3 16 GB DIMM (40)
		APC Smart-UPS 2200VA RM 2U LCD
	Mass Storage	Dell EqualLogic PS6000E Storage Area Network (SAN)
		Dell EqualLogic PS6000E SAN
		Dell EqualLogic PS6100X SAN
		LaCIE 8TB Network Attached Storage (NAS)
		LaCIE 4TB NAS
		LaCIE 4TB NAS
		Synology RS812 NAS
		Synology RS814 NAS
		Synology RS2418+ NAS
		Cisco Catalyst 3850-24T-L SAN Switch
		Western Digital Red 3TB NAS hard drive (14)
	Network Device	Juniper SSG-140 VPN
	Workstation	Dell Latitude E5570
		Dell Latitude E5570
		Dell Latitude E5570
		Dell Latitude E5570

Software		Dell Latitude E5570
		Dell Latitude E5570
		SCM SCR331 Smart Card Reader (10)
	Operating System	Microsoft Windows Server 2012 R2 Standard (5 server)
		RedHat Enterprise Linux (2)
		Microsoft Windows 10 Professional (8)
	Database	Microsoft SQL Server 2014 Enterprise (4 core)
	Tool	Solarwinds Server & Application Monitor
		Solarwinds Network Performance Monitor
		Splunk Enterprise Annual (2 GB/day)
		Symantec Anti-Virus Endpoint Protection (SEP)-Windows (60)
		Symantec Anti-Virus SEP-Linux (2)
		Microsoft Visual Studio Enterprise
		Microsoft Visual Studio Professional (12)
		PragmaticWorks Task Factory
		PragmaticWorks Doc xPress Pro
		Sparx Systems Enterprise Architect
		Redgate SQL Data Compare Professional (2)
		WinZip Standard (2)

6.2 Data Access Controls. The Contractor shall ensure that the systems in this PWS are capable of limiting access to information based on the customers need to know. The systems shall be able to sustain several thousand hits and concurrent queries with no degradation. FR2 shall be available 24 hours per day, seven (7) days per week. Response time must meet Government expectations. The Contractor shall ensure that the systems allow authorized users to easily change what information users can view or update.

6.3 Other Compliance. The Contractor shall comply with Federal, Privacy, and other data directives as follows:

- Health Insurance Portability and Accountability Act (HIPAA)
- DoD 6025.18-R "Department of Defense Health Information Privacy Regulation," January 24, 2003, as a DoD Business Associate
- Applicable HIPAA Privacy and Security requirements regarding health information as defined in the TMA BAA and in DoD 6025.18-R and DoD 8580.02-R, as amended
- Applicable rules and policies governing data usage, storage, and maintenance:
 - DoDI 6055.07, DoD Accident Investigation, Reporting, and Record Keeping
 - DoD Net Centric Data Strategy
 - Memoranda of Understanding (provided upon task award)
 - Data Use Agreements (provided upon task award)
 - OSHA requirements for lost work day data collection
 - Service specific mishap reporting requirements

6.4 Foreign Travel. If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the SSC Pacific foreign travel team, Topside, Building 27, 2nd Floor - Room 206 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 40

days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one (1) year of departure and a country specific briefing within 90 days of departure.

Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and Contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at: <https://atlevel1.dtic.mil/at/>

Contact SSC_PAC_SECURITY_TRAINING@NAVY.MIL if problems are encountered accessing this website. Forward a copy of the training certificate to the previous email address or fax to (619) 553-6863.

6.5 Place of Performance. The work under this task order is to be performed at Government sites and at the Contractor's facility. The Government anticipates 90% of the work to be performed at the Contractor's facility or off-site, 10% at the Government site, Pentagon, Washington, D.C. 20301-4000. Work may be performed at other Government and Contractor sites as approved and deemed necessary by the Government.

6.6 Inspection and Acceptance. All deliverables shall be delivered to USD (P&R), Personnel Risk Reduction for inspection by the Government technical coordinator and acceptance by the Contracting Officer's Representative (COR).

6.7 Intellectual Property and Data Rights. All intellectual property derived and resulting from this project shall be Government property, unless otherwise specified by the Government. All data collected and analyzed data shall be Government property.

6.8 Deliverables.

- Monthly Status Report (CDRL A001)
- Report, Record of Meetings/Minutes (CDRL A004)
- Technical Report – Study/Services (CDRL A005)
- Contractor Roster (CDRL A015)

6.9 Point of Contacts. Points of contacts for this effort are:

Technical Representative - To be determined at time of award.

Technical Coordinator - To be determined at time of award.

7.0 PERFORMANCE BASED CRITERIA

7.1 Performance Requirement. The Contractor shall provide services and deliverables in accordance with this PWS and in accordance with the attached task order Contract Data Requirements List (CDRL) DD Form 1423-1 items.

7.2 Performance Standard. The Contractor's performance shall meet all of the requirements of this PWS and comply with all applicable guidance, directives, and standards. The Contractor shall deliver all task order data items in accordance with the authorities, content, format, media, marking, applications, quantities, frequency and submission date, delivery method, addressee, and DD250 requirements specified in the CDRL for each data item.

7.2 Acceptable Quality Level. The effectiveness of the Contractor's deliverables and services shall be measured for 100% compliance with all PWS and CDRL requirements. The Government shall evaluate (1) the quality of services and deliverables in terms of the Contractor's compliance with the performance standard, (2) the Contractors' timeliness with respect to task order, milestones, and delivery schedules, (3) the Contractor's cost control in terms of effectiveness in forecasting, managing, and controlling cost, and (4) the Contractor's business relations in terms of timeliness, completeness, quality of problem identification and corrective action, and reasonable and cooperative behavior.

Contracting Officer's Representative - To be determined at time of award.